United States District Court

EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

RICHARD SMITH and SHAE LOFTICE on behalf of themselves and all others similarly situated,	§	
Plaintiffs,	§	Civil Action No. 4:23-cv-295
v.	§	Judge Mazzant
AMERICAN PAIN AND WELLNESS, PLLC	§	
Defendant.	§	

MEMORANDUM OPINION AND ORDER

Pending before the Court is Plaintiffs' Motion to Compel (Dkt. #19). Having considered the Motion, the Response, the Reply, and the applicable law, the Court finds that Plaintiffs' Motion should be **GRANTED.**

BACKGROUND

This discovery dispute arises in the context of a class action lawsuit resulting from a purported data breach (Dkt. #4 at p. 1). Named Plaintiffs Richard Smith and Shae Loftice assert that American Pain and Wellness, PLLC's failure to secure highly sensitive personal identifiable information ("PII") and protected health information ("PHI") (collectively, "PII/PHI") allowed "cybercriminals [to] infiltrate[] its insufficiently protected computer systems in a data breach" (Dkt. #4 at p. 1). Plaintiffs contend that the data breach constituted an invasion of their privacy, causing a diminution in the value of their PII/PHI and exposing them to a greater risk of identity theft (Dkt. #4 at pp. 8–9). Consequently, Plaintiffs purport to suffer from "anxiety, sleep disruption, stress, fear, and frustration" (Dkt. #4 at pp. 8, 10).

On April 24, 2023, Plaintiffs filed their Amended Class Action Complaint (Dkt. #4). Plaintiffs bring their Class Action Complaint on behalf of themselves and all others harmed by Defendant's alleged misconduct (Dkt. #4 at p. 2). According to Plaintiffs, the other members of the putative class are current and former patients of Defendant whose data was accessed in the data breach, and who subsequently received breach notices (Dkt. #4 at p. 2). Defendant moved to dismiss Plaintiffs' Complaint on May 18, 2023, on grounds that the Court lacked subject matter jurisdiction, Plaintiffs lacked standing to bring their claims, and Plaintiffs failed to state a claim upon which relief may be granted (Dkt. #8). While Defendant's Rule 12(b)(1) and (6) Motions to Dismiss were pending, this discovery dispute ensued (Dkt. #8). On July 29, 2024, the Court held a teleconference to resolve the dispute. However, during the teleconference, Defendant cited the Court's supposed lack of jurisdiction as a basis for resisting discovery. Having determined that the Court has subject matter jurisdiction over this case—thereby denying Defendant's Motion to Dismiss—the Court will now address the discovery dispute (Dkt. #32).

Broadly speaking, Plaintiffs seek discovery to identify four categories of information. First, they seek information about the potential victims of the data breach (Dkt. #20-1 at p. 5; Dkt. #20-2 at p. 5). Second, Plaintiffs seek information related to Defendant's cybersecurity risks, policies, training, and budget (Dkt. #20-1 at pp. 6–9). Third, they seek to discover information related to the data breach itself and potential PII/PHI accessed by cybercriminals (Dkt. #20-2 at pp. 7–8). Fourth and finally, Plaintiffs seek to discover Defendant's communications with patients related to cybersecurity, including remedial measures taken after the data breach (Dkt. #20-1 at p. 6; Dkt. #20-2 at pp. 6, 8–9). Plaintiffs contend that Defendant has not been forthcoming in responding to discovery requests (*See* Dkt. #19). As a result, the parties "are at an impasse on Interrogatory Nos.

1, 2, 5, 10, 13, and 14, and Request Nos. 1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 21, and 22" (Dkt. #19 at p. 1; Dkt. #20-3; Dkt. #20-4). The parties also disagree on whether Plaintiffs are entitled to depose Plaintiff Smith's treating physician, Dr. Kamlesh Sisodiya (Dkt. #19 at p. 6; Dkt. #23 at pp. 3–4). In an effort to resolve the impasse, Plaintiffs filed this Motion to Compel on October 30, 2023 (Dkt. #19). Defendant filed a Response (Dkt. #23) and Plaintiffs filed a Reply (Dkt. #24).

LEGAL STANDARD

Under Federal Rule of Civil Procedure 26(b)(1), parties "may obtain discovery regarding any non[-]privileged matter that is relevant to any party's claim or defense . . . ." FED. R. CIV. P. 26(b)(1). "Information within this scope of discovery need not be admissible in evidence to be discoverable." FED. R. CIV. P. 26(b)(1). The Court's scheduling order requires that the parties produce, as part of their initial disclosure, "documents containing, information 'relevant to the claim or defense of any party'" (Dkt. #15 at p. 2). Moreover, the Local Rules of the Eastern District of Texas provide further guidance suggesting that information is "relevant to any party's claim or defense [if]: (1) it includes information that would not support the disclosing parties' contentions; . . . (4) it is information that deserves to be considered in the preparation, evaluation or trial of a claim or defense. . . ." LOCAL RULE CV-26(d). It is well established that "control of discovery is committed to the sound discretion of the trial court." *Freeman v. United States*, 556 F.3d 326, 341 (5th Cir. 2009) (quoting *Williamson v. U.S. Dep't of Agric.*, 815 F.2d 368, 382 (5th Cir. 1987)).

Rule 37 of the Federal Rules of Civil Procedure allows a discovering party, on notice to other parties and all affected persons, to "move for an order compelling disclosure or discovery." FED. R. CIV. P. 37(a)(1). The moving party bears the burden of showing that the materials and

information sought are discoverable. *Export Worldwide, Ltd. v. Knight*, 241 F.R.D. 259, 263 (W.D. Tex. 2006). Once the moving party establishes that the materials requested are within the scope of permissible discovery, the burden shifts to the party resisting discovery to show why the discovery is irrelevant, overly broad, unduly burdensome or oppressive, and thus should not be permitted. *Id.*

Federal Rule of Civil Procedure 34 governs requests for production of documents, electronically stored information, and tangible things. Rule 34 requires responses to "either state that inspection and related activities will be permitted as requested or state with specificity the grounds for objecting to the request, including the reasons." FED. R. CIV. P. 34(b)(2)(B). "An objection [to the entire request] must state whether any responsive materials are being withheld on the basis of that objection." FED. R. CIV. P. 34(b)(2)(C). On the other hand, "[a]n objection to part of a request must specify the part and permit inspection of the rest." FED. R. CIV. P. 34(b)(2)(C).

After responding to each request with specificity, the responding attorney must sign their request, response, or objection certifying that the response is complete and correct to the best of the attorney's knowledge and that any objection is consistent with the rules and warranted by existing law or a non-frivolous argument for changing the law. FED. R. CIV. P. 26(g). This rule "simply requires that the attorney make a reasonable inquiry into the factual basis of his response, request, or objection." FED. R. CIV. P. 26(g) advisory committee note (1983).

The federal rules follow a proportionality standard for discovery. FED. R. CIV. P. 26(b)(1). Under this requirement, the burden falls on both parties and the court to consider the proportionality of all discovery in resolving discovery disputes. FED. R. CIV. P. 26(b)(1), advisory

committee note (2015). This rule relies on the fact that each party has a unique understanding of the proportionality to bear on the particular issue. *Id.* For example, a party requesting discovery may have little information about the burden or expense of responding. *Id.* "The party claiming undue burden or expense ordinarily has far better information—perhaps the only information—with respect to that part of the determination." *Id.*

ANALYSIS

The parties have identified six discovery disputes that remain ripe for the Court's review (Dkt. #19 at p. 6; Dkt. #23 at p. 2). First, Plaintiffs assert that Defendant refuses to provide "class" discovery (Dkt. #19 at p. 6). Second, the parties disagree as to the temporal scope of discovery (Dkt. #19 at p. 6). Third, Defendant resists production of certain documents because it contends that no PII/PHI was accessed in the data breach (Dkt. #19 at p. 6). Fourth, Plaintiffs maintain that Defendant has too narrow a view of which cybersecurity measures are relevant to Plaintiffs' claims (Dkt. #19 at p. 6). Fifth, Defendant objects to one of Plaintiffs' discovery requests as vague and ambiguous (Dkt. #19 at p. 6). Sixth and finally, Plaintiffs seek to compel the deposition of Dr. Kamlesh Sisodiya, while Defendant alleges that Dr. Sisodiya's deposition would be "unnecessary and harassing" (Dkt. #19 at p. 6; Dkt. #23 at p. 3–4). The Court addresses each issue in turn.

I. "Class" Discovery: Request Nos. 1, 4, 22, and Interrogatory Nos. 2 and 5

In Request Nos. 1, 4, and 22, Plaintiffs seek to discover the number of patients whose data was accessed in the data breach, representations made to current and former patients concerning data protection and security, and reports of suspicious activity from patients after the data breach (Dkt. #20-3 at pp. 1, 3, 10). In Interrogatory Nos. 2 and 5, Plaintiffs request the citizenship of data breach victims for class certification purposes, as well as any representations Defendant made to

data breach victims regarding data protection and security in Defendant's systems (Dkt. #20-4 at pp. 2–3). Defendant objects to these Requests and Interrogatories by asserting that only discovery about the two named Plaintiffs is relevant at this stage (*See* Dkt. #20-3 at pp. 1, 3, 10; Dkt. #20-4 at pp. 2–3). The Court disagrees and instead finds that Plaintiffs have established a right to any documents that Defendant has yet to produce related to the Requests and Interrogatories listed above.

In short, the Court agrees with Plaintiffs' position that the requests above seek information relevant for class certification, jurisdictional questions, and damages analyses (Dkt. #19 at p. 7). Defendant claims that its discovery obligations extend only to the named plaintiffs (Dkt. #23 at p. 2). Therefore, according to Defendant, any information related to the putative class is irrelevant, rendering it undiscoverable (Dkt. #23 at p. 3).[1] But Defendant views Rule 26's relevance standard through too narrow a lens. FED. R. CIV. P. 26. Under Rule 26, relevant information includes "any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case." FED. R. CIV. P. 26; *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978) (citing *Hickman v. Taylor*, 329 U.S. 495, 501 (1947)). Further, as Plaintiffs correctly observe, "class certification discovery is not limited to named plaintiffs—which would defeat the purpose of class certification discovery—but to facts that are relevant to class certification issues" (Dkt. #19 at p. 8) (quoting *Morrow v. City of Tenaha Deputy City Marshal Barry Washington*, No. 2-

[1] During the discovery teleconference on July 29, 2024, Defendant challenged the Court's subject matter jurisdiction over this action, citing the "home state" exception to the Class Action Fairness Act (CAFA). Hearing on Plaintiffs' Motion for Schedule Extension at 2:18:00 p.m.; 28 U.S.C. § 1332(d)(4) (providing that the court must abstain from exercising jurisdiction if two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the state in which the action was originally filed). Ironically, in order to determine if the home state exception to CAFA jurisdiction applies, discovery is necessary to determine the citizenship of the 7,457-member putative class. Because Defendant has resisted discovery related to the citizenship of the putative class, the Court cannot determine whether the home state exception applies. In any event, Defendant has not yet briefed the Court on whether this exception applies.

08-cv-288-TJW, 2010 U.S. Dist. LEXIS 67809, at *10 (E.D. Tex. July 7, 2010)). Given that the information Plaintiffs seek in Request Nos. 1, 4, 22, and Interrogatory Nos. 2 and 5 bear on the issues of class certification, jurisdictional questions, and damages analyses, Plaintiffs have met the low bar for relevance under Rule 26.

Defendant also misconstrues the applicable burden scheme in the discovery process. Defendant contends that it is entitled to resist discovery using the following logic:

> [Defendant] maintains that it has no reason to believe that any of Plaintiffs' (or any potential class member's) PII/PHI was accessed or compromised as a result of the Data Breach. Unless and until [Defendant] is provided evidence otherwise, it is entitled to take this position.

(Dkt. #23 at p. 2). In effect, Defendant's argument would require Plaintiffs to establish a *prima facie* case in order to participate in discovery (Dkt. #23 at p. 2). Not so. The Federal Rules simply place an initial burden on the party seeking discovery to establish relevance, after which the party *resisting* discovery bears the burden of showing specifically how each discovery request is *not* relevant. *See McLeod, Alexander, Power & Apffel, P.C. v. Quarles*, 894 F.2d 1482, 1485 (5th Cir. 1990). Defendant has not met this burden. Further—and perhaps more importantly—Defendant cannot shield itself from its discovery obligations by denying liability. Certainly, if the Federal Rules permitted parties to resist discovery for what they believe to be meritless claims, then no documents would ever be produced. Indeed, no case would ever make it before a jury.

Finally, in its Response to Plaintiffs' Motion to Compel, Defendant contends that it produced supplemental responses to Plaintiffs' Requests for Production and Interrogatories on November 13, 2023 (Dkt. #23 at p. 6). Defendant thus argues that the discovery issues regarding Request Nos. 1 and 4, and Interrogatory Nos. 2 and 5, are now resolved and moot (Dkt. #23 at p. 6). However, Plaintiffs maintain that Defendant never provided any supplemental responses (Dkt.

#24 at pp. 1–2). To date, the Court is not aware of any supplemental responses that would render these discovery disputes moot.

The Court concludes that the documents and responses sought by Plaintiffs are relevant and proportional to this case. Of course, the Court cannot compel a party to produce materials that do not exist. Nor can it compel a party to produce documents outside of its custody, possession, or control. *See* FED. R. CIV. P. 34(a) ("A party may serve on any other party a request . . . to produce . . . the following items in the responding party's *possession, custody, or control* . . . .") (emphasis added). Thus, the Court orders Defendant to produce or make available to Plaintiffs all unproduced documents responsive to Request Nos. 1, 4, and 22 that are in its possession, and to adequately respond to Interrogatory Nos. 2 and 5. To the extent that Defendant contends that it has no documents to produce, it must indicate to Plaintiffs whether it lacks possession, custody, or control of the documents, or alternatively, whether the requested documents do not exist or have already been produced. *See Bevill v. City of Quitman, Tex.*, No. 4:19-CV-00406, 2022 WL 14318439, at *7 (E.D. Tex. Oct. 24, 2022) (directing a party to provide supplemental responses to a request for production or otherwise provide the requesting party with an explanation for its inability to produce responsive documents).

II. Temporal Scope: Request Nos. 2, 3, 8, 15, and 17

The second discovery dispute before the Court centers around a disagreement between the parties regarding how far back in time before the data breach Plaintiffs may reach through their Requests and Interrogatories (Dkt. #19 at p. 8). Specifically, Request Nos. 2, 3, 8, 15, and 17 seek documents identifying the cybersecurity training, policies, and procedures that Defendant implemented to protect its patients' PII/PHI (Dkt. #20-1 at pp. 6–9). Defendant objects to each

request as overbroad because the requests are not limited in time (Dkt. #20-3 at pp. 2, 4, 7). According to Defendant, "[a]nything that occurred prior to the Data Breach or after the Data Breach will have no bearing on whether [Defendant] was liable to Plaintiffs for the Data Breach" (Dkt. #23 at p. 2). While the Court agrees with Defendant that Plaintiffs' requests are too broad because they lack a time limitation, the Court disagrees with Defendant about the relevant time period for these requests (Dkt. #23 at p. 2).

In opposition to Plaintiffs' Motion to Compel, Defendant maintains that "without any limitation in time or scope, this Request would be seeking *all* documents and communications for *all* time regarding *any* policies and/or procedures regarding the collection and retention of PII/PHI from patients" (Dkt. #23 at pp. 7–8). As a result, Defendant has produced only those documents that were in place on the date of the data breach (Dkt. #20-3 at pp. 2, 4, 7). But as Plaintiffs observe, the relevant and proportional time period for Defendant's policies and procedures for protecting its patients' PII/PHI extends beyond just the date of the data breach (Dkt. #24 at pp. 2–3). Not only that, but Plaintiffs contend that they have already unsuccessfully attempted to limit the time frame of the request (Dkt. #24 at pp. 2–3; Dkt. #20-7 at pp. 2–3).

Accordingly, the Court finds that the appropriate remedy is to modify each request to include a time limitation. On September 19, 2023, Plaintiffs supplemented their requests and interrogatories (Dkt. #20-7). Plaintiffs proposed reasonable time periods for certain requests, seeking documents from "November 1, 2020, through present" (Dkt. #20-7 at pp. 3–4). The Court finds that Plaintiffs' proposed time frame is relevant and proportional to the claims at issue. Therefore, the Court orders Defendant to produce documents responsive to Plaintiffs' Request Nos. 2, 3, 8, 15, and 17 from November 1, 2020, through September 19, 2023.

III. Access to PII/PHI: Request No. 1 and Interrogatory Nos. 1, 2, 10, and 13

Next, Defendant takes issue with Plaintiffs' Interrogatory Nos. 1, 2, 10, 13, and Request No. 1 (Dkt. #20-3 at pp. 1–2; Dkt. #20-4 at pp. 1–2, 6–7). Plaintiffs seek responses and documents identifying what information may have been accessed in the data breach, which patients had their data accessed, and whether that information was misused (Dkt. #20-3 at pp. 1–2; Dkt. #20-4 at pp. 1–2, 6–7). Defendant objected to these requests on the basis that "no PII/PHI was accessed by an unauthorized party during the Data Breach" (Dkt. #20-3 at pp. 1–2; Dkt. #20-4 at pp. 1–2, 6–7). In its Response to Plaintiffs' Motion to Compel, Defendant made the following argument:

> [Defendant] is not refusing to produce documents or information because it does not believe that any PII/PHI was accessed. Rather, [Defendant] properly responded to numerous written discovery requests stating that it does not believe any PII/PHI was accessed by the threat actors causing the Data Breach. . . . [Defendant] has no reason to believe that any PII/PHI was accessed as a result of the Data Breach.

(Dkt. #23 at pp. 2–3). That argument is circular and appears to make no real distinction. As Plaintiffs recognize, Defendant sent notices directly to the putative class members, informing them that their PII/PHI *was* accessed (Dkt. #24 at p. 3) (citing Dkt. #4 at p. 4 n.3). Moreover, and as the Court already addressed, Defendant cannot escape its discovery obligations by disclaiming liability. *See supra* Section I. Accordingly, the Court orders that Defendant provide fulsome responses to Interrogatory Nos. 1, 2, 10, and 13, and produce responsive documents to Request No. 1, to the extent that Defendant has any such documents in its possession, custody, or control.

IV. Relevant Cybersecurity Policies: Request Nos. 10, 11, 12, 13, 14, 16, and 21

The parties have also reached an impasse on Request Nos. 10, 11, 12, 13, 14, 16, and 21 (Dkt. #20-3 at pp. 5–7, 9). These requests seek documents related to the cybersecurity measures that Defendant employed to protect its patients' PII/PHI (Dkt. #19 at p. 9). Defendant's objections to

each request fall into two categories. First, Defendant raises a general objection to relevance, asserting that Plaintiffs seek "documents and tangible things that are not relevant to the claims or defenses of any party" (Dkt. #20-3 at pp. 5–7, 9). Second, Defendant argues that the only "cybersecurity measures that are at issue in this case are those that were in effect on the date of the Data Breach" (Dkt. #23 at p. 3). The Court will address each objection in turn.

Defendant's relevance objections misapply the relevance standard under Rule 26. Defendant claims that the following categories of information are not relevant to Plaintiffs claims: the identity of its cybersecurity vendors, cybersecurity budget, data security training, employee compliance with data security training, and the decision not to offer credit monitoring services to its patients as a result of the data breach (Dkt. #20-3 at pp. 5–7, 9). But "'[r]elevancy is broadly construed, and a request for discovery should be considered relevant if there is 'any possibility' that the information sought may be relevant to the claim or defense of any party.'" *Muhammed v. Shelton*, No. 4:23-CV-428, 2024 WL 3498346, at *1 (E.D. Tex. July 22, 2024) (quoting *S.E.C. v. Brady*, 238 F.R.D. 429, 437 (N.D. Tex. 2006)). Accordingly, "'[u]nless it is clear that the information sought can have no possible bearing on the claim or defense of a party, the request for discovery should be allowed.'" *Id.*

Here, Defendant's cybersecurity measures certainly have some "possible bearing" on Plaintiffs' claims. *See id.* Indeed, the adequacy of Defendant's cybersecurity infrastructure and training is at the heart of Plaintiffs' Complaint (Dkt. #4 at ¶5) (asserting that "Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI"). Therefore, the Court finds that Request

Nos. 10, 11, 12, 13, 14, 16, and 21 seek information that is relevant to Plaintiffs' claim (Dkt. #20-3 at pp. 5–7, 9).

The Court rejects Defendant's second objection for reasons already discussed in Section II above. *See supra* Section II. To reiterate, in short, Defendant insists that the scope of Plaintiffs' requests is too broad because, according to Defendant, the only relevant date for responsive documents is the date of the data breach itself (Dkt. #23 at p. 3). Relatedly, Defendant asserts that any documents that contemplate cybersecurity measures Defendant put in place *after* the data breach are not discoverable because they are subsequent remedial measures (Dkt. #23 at p. 3). Neither argument is availing.

As to Defendant's first argument, the Court agrees that the scope of Plaintiffs' request is too broad because it does not contain a reasonable time limitation but disagrees with Defendant's proposal that the request should be limited to the date of the data breach. Instead, the Court applies the same reasoning from Section II to calculate the applicable time frame for responsive documents. *See supra* Section II.

In its second argument, Defendant challenges the admissibility of the cybersecurity measures it had in place after the date of the data breach, citing the subsequent remedial measures defense (Dkt. #23 at p. 3). Under the Federal Rules of Evidence, evidence of subsequent remedial measures is not admissible to prove negligence, culpable conduct, a product or design defect, or the need for a warning or instruction. FED. R. EVID. 407. According to Defendant, Rule 407 protects all of Defendant's post-data breach cybersecurity policies from discovery. *Id.*; (Dkt. #23 at p. 3). But Defendant confuses discoverability for admissibility. Importantly, however, the Federal Rules of Civil Procedure distinguish between the two when defining the scope of discovery.

FED. R. CIV. P. 26(b)(1) ("Information within this scope of discovery need not be admissible in evidence to be discoverable"). The Court thus finds that the relevant time period for discovery extends after the date of the data breach. Hence, the Court orders Defendant to produce documents responsive to Plaintiffs' Request Nos. 10, 11, 12, 13, 14, 16, and 21 from November 1, 2020, through September 19, 2023.

V. Vague and Ambiguous: Request No. 7

Defendant next contests Request No. 7, which seeks "[a]ll documents regarding [Defendant's] compliance or noncompliance with any applicable data security guidelines or standards" (Dkt. #20-3 at p. 4). Defendant objects to this request as vague and ambiguous because "there is no way for [Defendant] to determine what documents it is being asked to produce" (Dkt. #20-3 at p. 4). The Court disagrees.

Even after a cursory review of Plaintiffs' Complaint, it is clear which standards Plaintiffs are referencing (Dkt. #4 at pp. 14–18). First, Plaintiffs contend that Defendant failed to follow FTC guidelines (Dkt. #4 at pp. 14–15) (citing *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (setting the guidelines for applicable data security principles and practices businesses must use to prevent and respond to data breaches)). Second, Plaintiffs aver that Defendant failed to follow applicable industry standards (Dkt. #4 at pp. 15–16) (discussing industry standards and best practices related to employee training and education, security software, authentication, malware detection, and cybersecurity frameworks). Third, Plaintiffs assert that Defendant violated HIPAA's security provisions and data privacy

responsibilities (Dkt. #4 at pp. 16–18) (collecting applicable HIPAA data privacy rules and safeguards to protect PII/PHI).

As written, Request No. 7 could be construed as vague and ambiguous when read in isolation. The Court recognizes that a more pointed request could have better alerted Defendant of the responsive documents to Plaintiffs' request. But discovery does not occur in a vacuum; it occurs in the broader context of the litigation. Here, Request No. 7 seeks documents responsive to Defendant's alleged violation of applicable standards—the same standards Plaintiffs included in their Complaint (Dkt. #20-3 at p. 4; Dkt. #4 at pp. 14–18). Therefore, in response to Request No. 7, the Court orders Defendant to produce documents related to Defendant's compliance or noncompliance with any applicable data security guidelines or standards defined in Plaintiffs' Complaint (Dkt. #4 at pp. 14–18).

VI. Deposition of Dr. Sisodiya

Finally, the parties disagree on whether Plaintiffs are entitled to depose Dr. Sisodiya, Smith's treating physician (Dkt. #19 at pp. 11–12; Dkt. #23 at pp. 3–4). Plaintiffs claim that Dr. Sisodiya's deposition is relevant because:

> Dr. Sisodiya called Mr. Smith, for the first time ever in their fifteen year doctor-patient relationship, to discuss not only the facts of the data breach (including the scope of what was breached generally and with respect to Mr. Smith specifically), and to threaten Mr. Smith with losing the medical treatment he has been receiving for years if he continues as a putative class representative in this case.

(Dkt. #19 at p. 11). Defendant, however, maintains that "Plaintiffs have no basis for compelling the deposition of Dr. Sisodiya" because "neither Plaintiffs nor [Defendant] have disclosed Dr. Sisodiya as a person with knowledge of relevant facts" (Dkt. #23 at p. 3). Therefore, according to

Defendant, "[Dr. Sisodiya's] deposition is outside the scope of discovery" (Dkt. #23 at p. 11) (citing FED. R. CIV. P. 26(b)(1)). The Court is not persuaded.

The Federal Rules provide that "[a] party may, by oral questions, depose *any* person, including a party, without leave of court . . . ." FED. R. CIV. P. 30(a)(1) (emphasis added). This is true irrespective of whether either party disclosed Dr. Sisodiya as a person with knowledge of relevant facts (Dkt. #23 at p. 11). Given the wide scope of discovery, "[i]t seems clear that the party seeking discovery is not required to establish that the person whose deposition it seeks has information about which he or she could testify at the trial." 8A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 2102 (3d ed. 2024). Indeed, one key purpose of discovery is to determine who possesses such information. *Id.* And, as Plaintiffs observe, Dr. Sisodiya has relevant knowledge about the data breach, as indicated by his suggestion that Smith speak with Defendant's employees Maxine Collins and Andrew Morgan about the data breach (Dkt. #19 at pp. 11–12). Dr. Sisodiya thus possesses information that would have *some* "possible bearing" on Plaintiffs' claim. *Muhammed v. Shelton*, No. 4:23-CV-428, 2024 WL 3498346, at *1 (E.D. Tex. July 22, 2024) (quoting *S.E.C. v. Brady*, 238 F.R.D. 429, 437 (N.D. Tex. 2006)). Consequently, the Court orders Defendant to produce Dr. Sisodiya for deposition.

CONCLUSION

It is therefore **ORDERED** that Plaintiffs' Motion to Compel (Dkt. #19) is **GRANTED.**

IT IS SO ORDERED.

SIGNED this 21st day of October, 2024.

AMOS L. MAZZANT
UNITED STATES DISTRICT JUDGE